ISSN (online) : 2277-5390
ISSN (Print) : 2277-5382

A survey on certificate revocation scheme using various approaches

R.R. Pavithra*[1], V. R. Nagarajan[2]

[1]*Student,* [2]*Assistant Professor, M.Phil in computer science, Sree Narayana Guru College, KG Chavadi, Coimbatore-641105, Tamil Nadu, India*
[1]pavithrasanjeev@gmail.com, [2]vrnag74@gmail.com

Abstract

The objectives of this survey is to analyse different certificate revocation approaches for identifying malicious attacks and to improve security. Certificate Revocation is a protection mechanism utilized to enhance the security level of network by detecting and removing malicious nodes from MANET with the help of certificate authority. There are different techniques used along with certificate revocation mechanism for recovering the nodes that are falsely accused by the neighborhood nodes. This paper provides detailed information of those mechanisms and finally compared their performance based on their merits and demerits.The finding of this work shows that clustering based revocation scheme is better than other mechanisms.

Keywords: certificate Revocation, MANET, topology, deployment.

1. Introduction

Self configuring network that contains randomly deployed mobile devices is commonly known as MANET. In such network, mobile devices are communicated through open medium and they move independently in any direction, and therefore frequently modify its links with respect to other devices. MANET has wide range of applications in military crisis, emergency instance and response operations. But presence of misbehavior nodes interrupted the transmission routing path that leads to the malfunctioning of network operations. Some of the malicious attacks try to corrupt the data's that are transmitted between different nodes where the some other attacks might attempt to change the path that they are transmitted to prevent valid node to receive the correct packets [1]. So security is considered as important concern in routing, network topology, and data traffic. Many researches have been carried out for providing security to the MANETs.

Certificate management mechanism is developed in which trust values are used for providing protection to services in the network and applications of network. Components like Prevention, Detection, and revocation are the security solutions utilized for certificate management. The task of adding and removing the certificates of attacks launching nodes is called certification revocation scheme. This revocation scheme has performed under voting based and non-voting based mechanism. Revocation of Certificate of attacker nodes through voting mechanism depends on the votes received by its non attacker nearby nodes. Nonvoting based revocation mechanism considered any given node as malicious attacker with a help of any other node that having valid certificate. There were various techniques developed in certificate revocation scheme. This paper will give brief explanation about those techniques and compared them based on the parameters utilized in the techniques.

In [2] designed the scheme for distributing the information of certificate revocation based on Square Residue and mathematical puzzle in certificate revocation. Real-time promulgation object was achieved by including current system time of certificate authority (CA) with the output message. By requests status validation of the user, the promulgation of certificate status was access driven and enhances the access stability.

In [3] developed a decentralized scheme for revoking the certificates of malicious nodes based on their weights. The proposed scheme makes use of certificates in accordance with hierarchical trust model and also gave all key management tasks to nodes that are deployed in the network. The malicious or attacker nodes were found at faster rate and the corresponding malicious nodes certificates were considered as an invalid.

In [4] proposed scheme for revoking the attacker's certificates within a limited operating traffic. The scheme makes use of the reliability of each node and form clusters for detecting false accusations. Attack detection and certificate recovery packets were utilized for inducing the Black List updation. There were five kinds of control packets utilized to revoke the malicious nodes. This scheme achieves lower operational traffic.

In [5] utilized certificate authority with trust counters for providing integrity of the network in addition with resisting attacks. The proposed three phase scheme consists of RCF packet monitoring, Certification revival and Certification revocation. RCF of packet monitoring continuously monitored the misbehaviour instances in the path of routing and packet forwarding in the network. While Certification revival and Certification revocation together used for providing privacy to the nodes. Privacy was based on the Shamir's secret sharing model with redundancy. This scheme results with less delay and overhead.

In [6] proposed Certificate Revocation scheme with Vindication Capability based on clustering for quick and accurate detection of malicious nodes. In this approach, false accusation was limited by cluster head (CH) for re-establishing the falsely revoked nodes. Here, Revoking of attacker node was depends on receiving the accusation from a neighboring node. This scheme minimizes the revocation time.

In [7] proposed the certificate revocation by clustering the nodes for quick revocation and recovering the attacker certificate and falsely accused certificate. The proposed scheme revokes the malicious device certificate at faster rate, stops the accessing of device to the network and enhances the network security. The loss of energy depends on the number of rounds.

In [8] proposed a certificate revocation scheme based on bloom filters in smart grid Advanced Metering Infrastructure (AMI) network. The size of Certificate Revocation Lists can be reduced by bloom filter in order to improve clusters' size with acceptable overhead. Two revocation schemes were proposed for addressing the false positive issue of the Bloom filter.

In [9]proposed an efficient certificate revocation scheme for pseudonymous public key infrastructure. Five certificate revocation schemes namely short-lived-certificate scheme, tamper-proof device scheme, online certificate status server scheme, certificate revocation list (CRL), and compressed CRL were utilized. It was proved that, one revocation scheme does not indulge the overhead and security of all smart grid applications.

In [10] proposed a signature scheme based on bilinear pairings for effective revoking of certificates of malicious nodes. This proposed scheme undergoes pairing operations in both the signing and verification phases. Here, Computational Diffie-Hellman (CDH) was applied to enhance the packet security to the network model. Proposed scheme can able to existentially unforgeable in opposition to adaptive chosen message and spot the malicious attacks by random oracle model.

In [11] introduced lightweight certificate revocation scheme for better efficiency and reliability in MANET. Scheme adapts the merits of voting based mechanism for allowing few nodes to involve in the revocation process for ensuring reliability. Acceleration strategy was proposed to reduce the number of voters needed for revoking a certificate. This scheme also provides vindication capability to tackle wrong certificate revocation. If the number of recovery packets was greater than the predefined number, the wrongly revoked node will be removed from Certificate Revocation Lists (CRLs).

2. Comparison tabulation

Ref. No.	Methods used	Merits	Demerits
2	Square Residue and mathematical puzzle	Save bandwidth, less computational complexity	Additional computational task is needed to reduce the work of operation
3	Decentralized scheme based on weighted accusation	Fast detection of false accusations	No guarantee for revocation of malicious nodes
4	Clustering	Traffic is low	Space complexity
5	Shamir's secret sharing model	overhead and time consumption get minimized	Flexibility is low while controlling and configuring certificates
6	Certificate Revocation scheme with Vindication Capability using clustering	revocation time get reduced	The scheme supports only uniformly distributed mobile nodes
7	Clustering	High accuracy, short revocation time	Unable to recover after corruption
8	Certificate revocation using Bloom Filters	High packet to delivery ratio	Space complexity, takes more time for computation
9	short-lived-certificate scheme, tamper-proof device scheme, online certificate status server scheme	Reduced overhead	Scalability issue
10	Computational Diffie-Hellman	Less computational and communicational cost	Does not considered about the side channel attacks
11	lightweight certificate revocation scheme based on Acceleration strategy	High accuracy of revocation, revocation time is less	High Communication overhead

3. Conclusion

Different techniques were developed with the certificate revocation scheme for effectively detecting the misbehaving nodes that cause different attacks in the network. The developed techniques should able to restore falsely accused nodes in a dynamic MANET environment. Finally, the best mechanism should be selected for enhancing the prediction accuracy. The finding of this work shows that clustering based revocation scheme is better than other mechanisms.

4. References

1. P. Rathiga. An Adaptive Identification and Prediction of Attacks in MANET: A Survey. Indian Journals of Innovations and Developments. 2015, 4(6), 1-6.
2. C.Lin, L.Huan-zhou, H.Yong. A digital certificate revocation status promulgation scheme based on square residue. In Proceedings Autonomous Decentralized Systems, ISADS 2005.IEEE, 208-211.
3. G.Arboit, C.Crépeau, C. R.Davis, M.Maheswaran. A localized certificate revocation scheme for mobile ad hoc networks. Ad Hoc Networks.2008, 6(1), 17-31.
4. K.Park, H.Nishiyama, N.Ansari, N.Kato. Certificate Revocation to Cope with False Accusations in Mobile Ad Hoc Networks. In VTC Spring. 2010, May, 1-5.
5. R.Ayyasamy, P.Subramani. An enhanced distributed certificate authority scheme for authentication in mobile ad-hoc networks. The International Arab Journal of Information Technology.2012, 9(3), 291-298.
6. W.Liu, H.Nishiyama, N.Ansari, J.Yang, N.Kato. Cluster-based certificate revocation with vindication capability for mobile ad hoc networks. IEEE Transactions on parallel and distributed systems. 2013, 24(2), 239-249.
7. Steven Raj, SnehaKathare. Clustering of Certificate Revocation to Reinforce an Idea for Mobile Ad Hoc Networks. International Journal of Engineering Research & Technology (IJERT), 2014, 3(7), 682-685.
8. K.Rabieh, M.Mahmoud, S.Tonyali. Scalable certificate revocation schemes for smart grid AMI networks using bloom filters. IEEE Transactions on Dependable and Secure Computing. PP(99), 1-1.
9. M. M.Mahmoud, J.Mišić, K.Akkaya, X.Shen. Investigating Public-Key Certificate Revocation in Smart Grid. IEEE Internet of Things Journal, 2015, 2(6), 490-503.
10. Y.Zhang, J.Li, Z.Wang, W.Yao. A New Efficient Certificate-Based Signature Scheme. Chinese Journal of Electronics.2015, 24(4), 776-782.
11. H.Xu, R.Wang, Z.Jia. A Lightweight Certificate Revocation Scheme for Hybrid Mobile ad Hoc Networks. International Journal of Security and Its Applications.2016, 10(1), 287-302.

The Publication fee is defrayed by Indian Society for Education and Environment (iSee). www.iseeadyar.org

Citation:

Pavithra R.R., V R Nagarajan. A survey on certificate revocation scheme using various approaches. *Indian Journal of Innovations and Developments.* 2016; 5 (5), May.